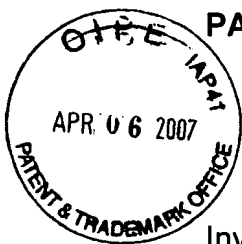


04-09-07

flw



**PATENT**

**Attorney Docket No: 738-X03-005**

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

Inventor: Hiroyasu YAMAMOTO et al  
Serial No.: 10/626,848  
Filed: July 23, 2003  
Art Unit: 2193  
Confirmation No.: 1886  
Title: RANDOM NUMBER GENERATOR AND PROBABILITY GENERATOR

**CERTIFICATE OF EXPRESS MAILING**

**PATENTS**

EXPRESS "Express Mail" Mailing Label number EV 968695447 US

Date of April 6, 2007

I hereby certify that the attached paper(s) or fee(s) is/are being deposited with the United States Postal Services "Express Mail Post Office to Addressee" service under 37 CFR §1.10 on the date indicated above and is addressed to the Commissioner for Patents, P. O. Box 1450, Alexandria, VA 22313-1450.

(Signature of person mailing paper or fee)

ESTEFANIA BELAUNDE

(Typed or printed name of person mailing paper or fee)

PATENT

Attorney Docket No: 738-X03-005

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants: Hiroyasu YAMAMOTO et al

Group Art Unit: 2193

Serial No.: 10/626,848

Confirmation No.: 1886

Filed: July 23, 2003

Examiner: Ngo, Choung D.

Title: RANDOM NUMBER GENERATOR AND PROBABILITY GENERATOR

SUBMISSION OF PRIORITY DOCUMENT

COMMISSIONER FOR PATENTS

P.O. Box 1450

Alexandria, VA 22313-1450

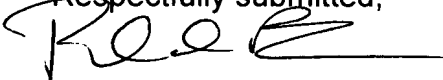
S I R :

Enclosed are a certified copies of the corresponding Japanese patent applications for which priority is claimed under 35 USC 119.

<u>Country</u>	<u>Application No.</u>	<u>Filing Date:</u>
JAPAN	2001-217710	July 18, 2001
JAPAN	2001-216704	July 17, 2001
JAPAN	2001-170945	June 6, 2001
JAPAN	2001-030833	February 7, 2001

No fee is believed to be due with this submission. However, if any fees are due, please charge any required fee (or credit any overpayments of fees) to the Deposit Account of the undersigned, Account No. 500601 (Docket No. 738-X03-005).

Respectfully submitted,



Paul D. Bianco, Reg. #43,500

Enclosures

Paul D. Bianco  
FLEIT KAIN GIBBONS GUTMAN BONGINI & BIANCO  
21355 E. Dixie Highway, Suite 115  
Miami, Florida 33180  
Tel: 305-830-2600; Fax: 305-830-2605  
E-mail: PBianco@FocusOnlp.com

(Translation)

PATENT OFFICE  
JAPANESE GOVERNMENT

This is to certify that the annexed is a true copy of the following application as filed with this Office.

Date of Application: June 6, 2001  
Application Number: No. 2001-170945  
Applicant: Iwaki Electronics Co., Ltd

Date: August 7, 2003  
Commissioner, Patent Office Yasuo IMAI (Seal)

Certificate No. 2003-3063564

日本国特許庁  
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日 2001年 6月 6日  
Date of Application:

出願番号 特願2001-170945  
Application Number:

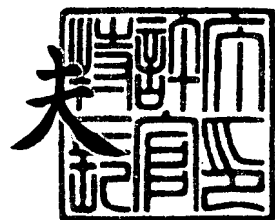
[ST. 10/C]: [JP 2001-170945]

願人 いわき電子株式会社  
Applicant(s):

2003年 8月 7日

特許庁長官  
Commissioner,  
Japan Patent Office

今井康夫



【書類名】 特許願

【整理番号】 IP01396

【あて先】 特許庁長官 殿

【国際特許分類】 H03K 3/84

【発明者】

【住所又は居所】 東京都港区新橋 5 丁目 3 6 番 1 1 号 いわき電子株式会社  
社内

【氏名】 山本 博康

【発明者】

【住所又は居所】 東京都港区新橋 5 丁目 3 6 番 1 1 号 いわき電子株式会社  
社内

【氏名】 アナンダ ビターナゲ

【発明者】

【住所又は居所】 東京都港区新橋 5 丁目 3 6 番 1 1 号 いわき電子株式会社  
社内

【氏名】 清水 隆邦

【発明者】

【住所又は居所】 東京都港区新橋 5 丁目 3 6 番 1 1 号 いわき電子株式会社  
社内

【氏名】 鯉淵 美佐子

【特許出願人】

【識別番号】 390022792

【氏名又は名称】 いわき電子株式会社

【代理人】

【識別番号】 100067046

【弁理士】

【氏名又は名称】 尾股 行雄

【電話番号】 03-3543-0036

## 【選任した代理人】

【識別番号】 100096862

## 【弁理士】

【氏名又は名称】 清水 千春

【電話番号】 03-3543-0036

## 【手数料の表示】

【予納台帳番号】 008800

【納付金額】 21,000円

## 【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 乱数発生装置および確率発生装置

【特許請求の範囲】

【請求項 1】 フリップ・フロップに入力する二つの入力信号の位相差を自動調整してフリップ・フロップ出力の 1 または 0 の出現率が一定になるようにした乱数発生装置において、

前記フリップ・フロップの入力ラインに、ノイズ発生源と、当該ノイズを増幅する増幅回路と、当該増幅ノイズ信号により入力信号にジッタを生じさせるミキサー回路とから構成されるジッタ生成回路を付加したことを特徴とする乱数発生装置。

【請求項 2】 前記フリップ・フロップの双方の入力ラインに前記ジッタ生成回路を付加したことを特徴とする請求項 1 に記載の乱数発生装置。

【請求項 3】 前記フリップ・フロップの何れか片方の入力ラインに前記ジッタ生成回路を付加し、他方の入力ラインに遅延時間補正用の積分回路を付加したことを特徴とする請求項 1 に記載の乱数発生装置。

【請求項 4】 前記ジッタ生成回路の出力を前記入力信号の繰り返し周期毎にラッチするラッチ手段を有することを特徴とする請求項 1 から請求項 3 までの何れかに記載の乱数発生装置。

【請求項 5】 二つの入力信号の位相差を自動調整してフリップ・フロップ出力の 1 または 0 の出現率が一定になるようにした乱数発生装置において、

前記フリップ・フロップのデータ入力ラインに、前記二つの入力信号の位相差を電圧に変換する位相－電圧変換回路を付加したことを特徴とする乱数発生装置。

【請求項 6】 前記位相－電圧変換回路は、動作許容時のみ作動するイネーブル手段を有することを特徴とする請求項 5 に記載の乱数発生装置。

【請求項 7】 前記位相－電圧変換回路の出力に、ノイズ発生源と、当該ノイズを増幅する増幅回路と、当該増幅ノイズ信号により入力信号にジッタを生じさせるミキサー回路とから構成されるジッタ生成回路を付加したことを特徴とする請求項 5 または請求項 6 の何れかに記載の乱数発生装置。

【請求項 8】 前記ジッタ生成回路は、動作許容時のみ作動するイネーブル手段を有することを特徴とする請求項 1 から請求項 4 および請求項 7 の何れかに記載の乱数発生装置。

【請求項 9】 前記ミキサー回路は、積分回路と、当該積分出力信号および前記増幅ノイズ信号をそれぞれ入力とする直列 P チャンネルトランジスタ回路と直列 N チャンネルトランジスタ回路の直列接続回路とで構成されることを特徴とする請求項 1 から請求項 4 および請求項 7 の何れかに記載の乱数発生装置。

【請求項 10】 前記ミキサー回路は、また、前記増幅ノイズ信号と前記入力信号の合成信号を入力とする N チャンネルトランジスタと P チャンネルトランジスタの直列トランジスタ回路で構成されることを特徴とする請求項 1 から請求項 4 および請求項 7 の何れかに記載の乱数発生装置。

【請求項 11】 R-S フリップフロップに入力する二つの入力信号の位相差を自動調整してフリップ・フロップ出力の 1 または 0 の出現率が一定になるようにした乱数発生装置において、

前記 R-S フリップ・フロップを構成する内部トランジスタ回路の R 側ゲート回路、もしくは S 側ゲート回路の電源側に P チャンネルトランジスタを、また GND 側に N チャンネルトランジスタを各々直列に接続すると共に、前記 P チャンネルトランジスタと N チャンネルトランジスタの入力にノイズ発生源と当該ノイズを増幅する増幅回路を接続し、当該増幅ノイズ信号により一方の前記ゲート回路のスレッシュホールド電圧を変化することを特徴とする乱数発生装置。

【請求項 12】 R-S フリップフロップに入力する二つの入力信号の位相差を自動調整してフリップ・フロップ出力の 1 または 0 の出現率が一定になるようにした乱数発生装置において、

前記 R-S フリップ・フロップを構成する内部トランジスタ回路の R 側ゲート回路、および S 側ゲート回路の電源側に P チャンネルトランジスタを、また GND 側に N チャンネルトランジスタを各々直列に接続すると共に、前記 P チャンネルトランジスタと N チャンネルトランジスタの入力にノイズ発生源と、当該ノイズを増幅する増幅回路を接続し、当該増幅ノイズ信号により双方の前記ゲート回路のスレッシュホールド電圧を変化することを特徴とする乱数発生装置。



【請求項 13】 前記増幅回路は、コンデンサと抵抗による直列入力回路と、PチャンネルトランジスタとNチャンネルトランジスタの直列回路とで構成され、且つ、当該トランジスタ回路の入力ー出力間に抵抗を介在したことを特徴とする請求項 1 から請求項 4 および請求項 7 および請求項 11 および請求項 12 の何れかに記載の乱数発生装置。

【請求項 14】 前記増幅回路は、また、コンデンサと抵抗による直列入力回路と、PチャンネルトランジスタとNチャンネルトランジスタの直列回路とで構成され、且つ、当該トランジスタ回路の入力ー出力間に抵抗とコンデンサを並列に介在したことを特徴とする請求項 1 から請求項 4 および請求項 7 および請求項 11 および請求項 12 の何れかに記載の乱数発生装置。

【請求項 15】 前記増幅回路を多段直列に接続して成る請求項 13 または請求項 14 の何れかに記載の乱数発生装置。

【請求項 16】 前記ノイズ発生源は、PチャンネルトランジスタとNチャンネルトランジスタを直列に接続すると共に、入力ー出力間を短絡して構成されることを特徴とする請求項 1 から請求項 4 および請求項 7 および請求項 11 および請求項 12 の何れかに記載の乱数発生装置。

【請求項 17】 前記ノイズ発生源は、また、PチャンネルトランジスタとNチャンネルトランジスタを直列に接続すると共に、入力ー出力間に抵抗を介在して構成されることを特徴とする請求項 1 から請求項 4 および請求項 7 および請求項 11 および請求項 12 の何れかに記載の乱数発生装置。

【請求項 18】 前記ノイズ発生源は、また、PチャンネルトランジスタとNチャンネルトランジスタを直列に接続し、入力ー出力間に抵抗を介在すると共に、入力ーGND間に抵抗とコンデンサによる直列回路を介在して構成されることを特徴とする請求項 1 から請求項 4 および請求項 7 および請求項 11 および請求項 12 の何れかに記載の乱数発生装置。

【請求項 19】 前記ノイズ発生源は、また、PチャンネルトランジスタとNチャンネルトランジスタを直列に接続し、入力ー出力間に抵抗を介在すると共に、入力ー電源間に抵抗とコンデンサによる直列回路を介在して構成されることを特徴とする請求項 1 から請求項 4 および請求項 7 および請求項 11 および請求

項 1 2 の何れかに記載の乱数発生装置。

【請求項 2 0】 前記ノイズ発生源は、また、Nチャンネルトランジスタの入力－出力間を短絡すると共に、出力－電源間に抵抗を介在して構成されることを特徴とする請求項 1 から請求項 4 および請求項 7 および請求項 1 1 および請求項 1 2 の何れかに記載の乱数発生装置。

【請求項 2 1】 前記ノイズ発生源は、また、Nチャンネルトランジスタの入力－出力間と出力－電源間にそれぞれ抵抗を介在して構成されることを特徴とする請求項 1 から請求項 4 および請求項 7 および請求項 1 1 および請求項 1 2 の何れかに記載の乱数発生装置。

【請求項 2 2】 前記ノイズ発生源は、また、Pチャンネルトランジスタの入力－出力間を短絡すると共に、出力－GND間に抵抗を介在して構成されることを特徴とする請求項 1 から請求項 4 および請求項 7 および請求項 1 1 および請求項 1 2 の何れかに記載の乱数発生装置。

【請求項 2 3】 前記ノイズ発生源は、また、Pチャンネルトランジスタの入力－出力間と出力－GND間にそれぞれ抵抗を介在して構成されることを特徴とする請求項 1 から請求項 4 および請求項 7 および請求項 1 1 および請求項 1 2 の何れかに記載の乱数発生装置。

【請求項 2 4】 請求項 1 から請求項 2 3 までの何れかに記載の乱数発生装置を用いて構成されることを特徴とする確率発生装置。

#### 【発明の詳細な説明】

#### 【0001】

#### 【発明の属する技術分野】

本発明は、科学技術計算、ゲーム機、或いは暗号化処理等に利用して好適な乱数発生装置、およびこの乱数発生装置を使用して構成した確率発生装置に関するものである。

#### 【0002】

#### 【従来の技術】

高度な科学技術計算やゲーム機、或いは暗号化処理等には乱数の使用が不可欠であり、近年、一様性（乱数の確率値および出現率に差異が生じないこと）を有

し、且つ、乱数出現の規則性、前後の相関性、周期性等を有しない高性能な自然乱数（真性乱数）の発生装置や確率発生装置の需要が益々増加してきている。

#### 【0003】

そして、上記した自然乱数／確率発生装置としては、例えば、微弱放射線、抵抗やダイオードの熱雑音、或いは水晶発振器の揺らぎ等を利用して得られるランダムなパルスを利用したものが公知である。

#### 【0004】

##### 【発明が解決しようとする課題】

ところで、上記した自然現象によるランダムパルスを利用した従来の乱数／確率発生回路においては、前記ランダムパルスの発生源、信号の増幅器、波形整形、一様性の適正化回路等のアナログ的要素が多分に含まれることから回路規模も大きく、且つ複雑となり、よって、これらを一体のロジック L S I として搭載することは難しく、今後需要増が期待される I C カード等のような超小型、薄型ハイテク機器への適用に対しても極めて不利であり、且つまた、L S I 化が困難であることから生産性が悪く、コスト的にも高くなるという問題を有していた。

#### 【0005】

本発明は、上記従来技術の問題を解消し、L S I 搭載に適する小型、薄型化を実現し生産性に優れると共に、性能においても、一様性や規則性、相関性、周期性等の問題を生じない高性能な乱数発生装置および確率発生装置を提供することを目的としている。

#### 【0006】

##### 【課題を解決するための手段】

二つの入力部に入力される信号の位相差に応じて出力の状態（1または0）が確定するフリップ・フロップとしてDタイプフリップ・フロップが公知である。

このDタイプフリップ・フロップは、図34に示すように、入力部となるクロック端子C L Kとデータ端子Dを有し、C L K入力信号の立ち上がり時のデータ端子Dの状態（0か1）によって出力Qと/Q（/Q：Qの反転出力）の状態が確定する、所謂エッジトリガ型のフリップ・フロップである。

ここで、図35（a）、若しくは図35（b）の状態からC L K信号の立ち上

がり時間とD信号の立ち上がり時間の差（位相差） $\Delta t$ を0に近づけていくと、図35（c）に示すように、フリップ・フロップ出力 $Q_n$ 、 $\bar{Q}_n$ が不確定となる位相差の範囲が存在する。そして、このフリップ・フロップの不確定動作範囲は入力信号のジッタが大きくなる程拡がり、乱数の生成をより容易にする。

#### 【0007】

本発明は、上記入力信号のジッタを大きくし、その際のフリップ・フロップの不確定動作を積極的に利用して自然乱数を生成するものである。

#### 【0008】

すなわち、請求項1に記載の乱数発生装置は、フリップ・フロップに入力する二つの入力信号の位相差を自動調整してフリップ・フロップ出力の1または0の出現率が一定になるようにした乱数発生装置において、前記フリップ・フロップの入力ラインに、ノイズ発生源と、当該ノイズを増幅する増幅回路と、当該増幅ノイズ信号により入力信号にジッタを生じさせるミキサー回路とから構成されるジッタ生成回路を付加して構成される。

#### 【0009】

また、請求項2に記載の乱数発生装置は、前記フリップ・フロップの双方の入力ラインに前記ジッタ生成回路を付加して構成される。

#### 【0010】

また、請求項3に記載の乱数発生装置は、前記フリップ・フロップの何れか片方の入力ラインに前記ジッタ生成回路を付加し、他方の入力ラインに遅延時間補正用の積分回路を付加して構成される。

#### 【0011】

ここで、前記請求項1から請求項3に記載の構成では、フリップ・フロップに入力される入力信号にジッタが発生し、フリップ・フロップの不確定動作範囲が拡がる。これにより、一様性を有し、且つ規則性や相関性や周期性を有しないより完全な自然乱数を容易に生成することができるようになる。

#### 【0012】

また、請求項4に記載の乱数発生装置は、前記ジッタ生成回路の出力を前記入力信号の繰り返し周期毎にラッチするラッチ手段を付加して構成される。

本構成では、1回の乱数生成において1回の入力信号を得ることができ、乱数の生成動作が安定する。

#### 【0013】

また、請求項5に記載の乱数発生装置は、二つの入力信号の位相差を自動調整してフリップ・フロップ出力の1または0の出現率が一定になるようにした乱数発生装置において、前記フリップ・フロップのデータ入力ラインに、前記二つの入力信号の位相差を電圧に変換する位相－電圧変換回路を付加して構成される。

本構成では、位相－電圧変換回路の出力には、これに接続される半導体素子（例えば、図25ではバッファ）のスレッシュホールド電圧にほぼ等しい電圧が発生し、フリップ・フロップ出力の1または0の出現率が一定になるように二つの入力信号の位相差（即ち、位相－電圧変換回路の出力）が自動調整される。

#### 【0014】

また、請求項6に記載の乱数発生装置は、前記位相－電圧変換回路は、動作許容時のみ作動するイネーブル手段を付加して構成される。

本構成では、乱数が必要な時にのみ動作許可信号を発行することにより、回路の活性期間を自在に制限することができ、よって低電力化が図れる。

#### 【0015】

また、請求項7に記載の乱数発生装置は、前記位相－電圧変換回路の出力に、ノイズ発生源と、当該ノイズを増幅する増幅回路と、当該増幅ノイズ信号により入力信号にジッタを生じさせるミキサー回路とから構成されるジッタ生成回路を付加して構成される。

本構成では、フリップ・フロップ出力の1または0が出る確率の不確定要素が積極的に増加される。これにより、一様性を有し、且つ規則性や相関性や周期性を有しないより完全な自然乱数を容易に生成することができるようになる。

#### 【0016】

また、請求項8に記載の乱数発生装置は、前記ジッタ生成回路は、動作許容時のみ作動するイネーブル手段を付加して構成される。

本構成では、乱数が必要な時にのみ動作許可信号を発行することにより、回路の活性期間を自在に制限することができ、よって低電力化が図れる。

**【0017】**

また、請求項 9 に記載の乱数発生装置は、前記ミキサー回路は、積分回路と、当該積分出力信号および前記増幅ノイズ信号をそれぞれ入力とする直列 P チャンネルトランジスタ回路と直列 N チャンネルトランジスタ回路の直列接続回路とで構成される。

**【0018】**

また、請求項 10 に記載の乱数発生装置は、前記ミキサー回路は、また、前記増幅ノイズ信号と前記入力信号の合成信号を入力とする N チャンネルトランジスタと P チャンネルトランジスタの直列トランジスタ回路で構成される。

**【0019】**

また、請求項 11 に記載の乱数発生装置は、R-S フリップフロップに入力する二つの入力信号の位相差を自動調整してフリップ・フロップ出力の 1 または 0 の出現率が一定になるようにした乱数発生装置において、前記 R-S フリップ・フロップを構成する内部トランジスタ回路の R 側ゲート回路、もしくは S 側ゲート回路の電源側に P チャンネルトランジスタを、また GND 側に N チャンネルトランジスタを各々直列に接続すると共に、前記 P チャンネルトランジスタと N チャンネルトランジスタの入力にノイズ発生源と当該ノイズを増幅する増幅回路を接続し、当該増幅ノイズ信号により一方の前記ゲート回路のスレッシュホールド電圧を変化するように構成した。

**【0020】**

また、請求項 12 に記載の乱数発生装置は、R-S フリップフロップに入力する二つの入力信号の位相差を自動調整してフリップ・フロップ出力の 1 または 0 の出現率が一定になるようにした乱数発生装置において、前記 R-S フリップ・フロップを構成する内部トランジスタ回路の R 側ゲート回路、および S 側ゲート回路の電源側に P チャンネルトランジスタを、また GND 側に N チャンネルトランジスタを各々直列に接続すると共に、前記 P チャンネルトランジスタと N チャンネルトランジスタの入力にノイズ発生源と、当該ノイズを増幅する増幅回路を接続し、当該増幅ノイズ信号により双方の前記ゲート回路のスレッシュホールド電圧を変化するように構成した。

## 【0021】

R-S フリップ・フロップにおいて、R 側入力信号と S 側入力信号の立ち上がりの位相差を 0 に近づけるとメタステーブル現象が発生する。この現象が発生すると、フリップ・フロップ出力が確定するまでに時間を要し、一定時間後の出力状態は、0 か 1、またはスレッシュホールド電圧を保持、または発振状態の何れかとなる。ここで、請求項 11 および請求項 12 に記載の構成では、R 側および／または S 側ゲート回路のスレッシュホールド電圧を変化することにより、メタステーブル状態より即時に 1 または 0 の安定した状態にすることができる。そして、このフリップ・フロップ出力の 1 または 0 の出現率が一定になるように二つの入力信号の位相差が自動調整される。

## 【0022】

また、請求項 13 に記載の乱数発生装置は、前記増幅回路は、コンデンサと抵抗による直列入力回路と、P チャンネルトランジスタと N チャンネルトランジスタの直列回路とを有し、且つ、当該トランジスタ回路の入力ー出力間に抵抗を介在して構成される。

## 【0023】

また、請求項 14 に記載の乱数発生装置は、前記増幅回路は、コンデンサと抵抗による直列入力回路と、P チャンネルトランジスタと N チャンネルトランジスタの直列回路とを有し、且つ、当該トランジスタ回路の入力ー出力間に抵抗とコンデンサを並列に介在して構成される。

## 【0024】

また、請求項 15 に記載の乱数発生装置は、前記増幅回路を多段構成とした。

ここで、前記請求項 13 から請求項 15 に記載の構成では、後述のノイズ発生源に応じて Low Pass Filter や High Pass Filter の周波数特性を適宜設定すれば好適な特性の増幅器を実現できる。また、MOS トランジスタで構成すると、温度や電源変動の影響を少なくでき、安定した動作が得られる。

## 【0025】

また、請求項 16 に記載の乱数発生装置は、前記ノイズ発生源は、P チャンネルトランジスタと N チャンネルトランジスタを直列に接続すると共に、入力ー出

力間を短絡して構成される。

**【0026】**

また、請求項17に記載の乱数発生装置は、前記ノイズ発生源は、また、PチャンネルトランジスタとNチャンネルトランジスタを直列に接続すると共に、入力ー出力間に抵抗を介在して構成される。

**【0027】**

また、請求項18に記載の乱数発生装置は、前記ノイズ発生源は、PチャンネルトランジスタとNチャンネルトランジスタを直列に接続し、入力ー出力間に抵抗を介在すると共に、入力ーGND間に抵抗とコンデンサによる直列回路を介在して構成される。

**【0028】**

また、請求項19に記載の乱数発生装置は、前記ノイズ発生源は、PチャンネルトランジスタとNチャンネルトランジスタを直列に接続し、入力ー出力間に抵抗を介在すると共に、入力ー電源間に抵抗とコンデンサによる直列回路を介在して構成される。

**【0029】**

また、請求項20に記載の乱数発生装置は、前記ノイズ発生源は、Nチャンネルトランジスタの入力ー出力間を短絡し、出力ー電源間に抵抗を介在して構成される。

**【0030】**

また、請求項21に記載の乱数発生装置は、前記ノイズ発生源は、Nチャンネルトランジスタの入力ー出力間と出力ー電源間にそれぞれ抵抗を介在して構成される。

**【0031】**

また、請求項22に記載の乱数発生装置は、前記ノイズ発生源は、Pチャンネルトランジスタの入力ー出力間を短絡し、出力ーGND間に抵抗を介在して構成される。

**【0032】**

また、請求項23に記載の乱数発生装置は、前記ノイズ発生源は、Pチャンネル



ルトランジスタの入力ー出力間と出力ーGND間にそれぞれ抵抗を介在して構成される。

### 【0033】

ここで、前記請求項16から請求項23に記載の構成では、ノイズ発生源として活性状態にある回路素子（トランジスタ、抵抗、コンデンサ、またはこれらの組み合わせ）より発生する微弱な熱雑音を利用しているため、簡単な回路構成によって極めて安価に実現できるものである。

### 【0034】

また、請求項24に記載の確率発生装置は、請求項1から請求項23までの何れかに記載の乱数発生装置を用いて構成される。

本構成では、乱数発生装置は一様性を有し、規則性、相関性、周期性を有しない理想的な確率発生装置を実現できる。また、暗号通信等に用いれば、セキュリティに優れた通信が行える。

### 【0035】

#### 【発明の実施の形態】

以下、図1～図33に基づいて本発明に係る乱数発生装置および確率発生装置の実施形態を説明する。

### 【0036】

先ず、本発明の第1実施形態を説明すれば、図1に示すように、第1実施形態の乱数発生装置10は、1bitのシリアル乱数RNDを出力するフリップ・フロップ1と、当該フリップ・フロップ入力（CLK信号）間に位相差を与える2系統の遅延回路2、3と、各遅延回路2、3に対応して付加したジッタ生成回路4、4と、前記遅延回路3の遅延時間を調整する位相制御回路5とで概略構成されている。

### 【0037】

前記位相制御回路5は、CLK信号の所定の繰り返し周期を計測すると共に、この所定周期内におけるフリップ・フロップ出力（乱数データRND）の1または0の数を監視してその出現率が一定値（例えば、50%）に維持されるよう前記遅延回路3の遅延時間を自動調整するフィードバック制御を行い、結果的には

、図35(c)のようにフリップ・フロップ1に入力される二つの入力信号の位相差 $\Delta t$ を0に近づけていくように動作する。

尚、最終段に付加したフリップ・フロップ6は、乱数データRNDの出力タイミングをCLK信号に同期させるためのラッチ回路である。

#### 【0038】

ここで、前記フリップ・フロップ1としては、入力信号の位相差によって出力の状態(1または0)が確定するエッジトリガ型のフリップ・フロップが使用可能であり、本実施形態では、CLK端子とD端子を備えたDタイプフリップ・フロップを使用すると共に、以下に細述するジッタ生成回路4により、入力信号に位相ジッタを誘起して積極的に不確定動作を起こさせるようにした。

#### 【0039】

図3に示すように、前記ジッタ生成回路4は、ノイズ発生源7と、発生した微弱なノイズを電力増幅する増幅回路8と、増幅されたノイズ信号によって入力信号にジッタを生じさせるミキサー回路9とで構成されている。

#### 【0040】

図3のジッタ生成回路4に搭載されたミキサー回路9は、直列に接続したPチャンネルMOSトランジスタQ4、Q3の回路と直列に接続したNチャンネルMOSトランジスタQ2、Q1の回路同士を直列接続(カスケード接続)して構成されており、各直列トランジスタ回路の内、トランジスタQ4とQ1のゲートには前記増幅回路8の出力が接続されると共に、トランジスタQ3とQ2のゲートには、抵抗RとコンデンサCによる積分回路12の出力が接続されている。尚、入力INには前記遅延回路2若しくは遅延回路3の出力が接続される。

#### 【0041】

上記回路構成では、図5に示すように、増幅されたノイズ信号をトランジスタQ4とQ1のゲートに入力することにより、遅延CLK信号の積分出力波形に対するトランジスタQ3、Q2のスレッシュホールド電圧が変動し、出力OUTにジッタ $\Delta j$ が発生する。このジッタ $\Delta j$ の大きさが後段のフリップ・フロップ1の不確定動作範囲を大いに広げることになる。

#### 【0042】

また、ミキサ回路 9 としては、図 3 の実施形態の他、図 4 に示す構成も採用可能である。図 4 の実施形態は、P チャンネル MOS トランジスタ Q 2 と N チャンネル MOS トランジスタ Q 1 の直列回路で構成されており、各ゲートには、増幅回路 8 の出力と入力 I N からの遅延 C L K 信号がそれぞれコンデンサ C と抵抗 R を介して接続されている。

従って、上記回路構成では、増幅されたノイズ信号と遅延回路により位相調整された C L K 信号とがコンデンサ C にて合成されてトランジスタ Q 2, Q 1 のゲートに入力されることになり、図 3 の場合と同様にジッタ  $\Delta j$  を有する出力 O U T が得られる。

#### 【0043】

次に、前記ノイズ発生源 7 の構成を説明する。

図 6 ～図 13 はノイズ発生源 7 の具体的な回路例を示している。

図 6 は、P チャンネル MOS トランジスタ Q 2 と N チャンネル MOS トランジスタ Q 1 を直列に接続し、ゲートー出力間を短絡して構成したものである。また、図 7 は、図 6 においてゲートー出力間に抵抗 R 2 を介在したものである。また、図 8 は、P チャンネル MOS トランジスタ Q 2 と N チャンネル MOS トランジスタ Q 1 を直列に接続し、ゲートー出力間に抵抗 R 2 を介在すると共に、ゲートー G N D 間に抵抗 R 1 とコンデンサ C 1 による R C 直列回路を介在して構成したものである。また、図 9 は、図 8 において前記 R C 直列回路をゲートー電源間に介在して構成したものである。また、図 10 は、N チャンネル MOS トランジスタ Q 1 のゲートー出力間を短絡し、出力ー電源間に抵抗 R 1 を介在して構成したものである。また、図 11 は、図 10 においてゲートー出力間に抵抗 R 2 を介在して構成したものである。また、図 12 は、P チャンネル MOS トランジスタ Q 1 のゲートー出力間を短絡し、出力ー G N D 間に抵抗 R 1 を介在して構成したものである。また、図 13 は、図 12 においてゲートー出力間に抵抗 R 2 を介在して構成したものである。

#### 【0044】

上記実施例では、活性状態にある回路素子（トランジスタ、抵抗、コンデンサ、またはこれらの組み合わせ）で発生する微弱な熱雑音を利用し、安価なノイズ

源を実現している。また、外部ノイズや電源変動等の影響も少なく、安定した動作が得られると共に、放射線源を利用していないことから、環境に対する安全性に優れ、使い捨て等による廃棄処分に対する問題も発生しない。

#### 【0045】

次に、図14、図15に基づいて前記増幅回路8の構成を説明する。

図14に示す増幅回路8は、コンデンサC1と抵抗R1による直列入力回路（High Pass Filter）とPチャンネルMOSトランジスタQ2とNチャンネルMOSトランジスタQ1の直列回路とで構成されており、また、図15に示す増幅回路8は、図14において、帰還抵抗R2にコンデンサC2を並列接続してLow Pass Filterを形成した構成である。図示しないが、これら増幅回路8の入力INには前記したノイズ発生源7の出力が接続され、出力OUTは前記したミキサー回路9に接続される。

上記構成の増幅回路8では、既述したノイズ発生源7の各構成に応じて前記High Pass FilterやLow Pass Filterの特性が設定され、好適な特性の増幅器を実現している。

#### 【0046】

次に、図16～図22に基づいてジッタ生成回路4の具体的な回路構成を説明する。これらは、既述したノイズ発生源7、増幅回路8、およびミキサー回路9の組み合わせで構成されるものであって、以下に示すものはその内の体系的な例を示すものである。従って、本発明がこれらの回路例のみに限定されるものではないことは勿論である。

#### 【0047】

図16は、図3の構成によるジッタ生成回路4で、図6に示したノイズ発生源7と図14に示した増幅回路8の組み合わせで構成されている。また、図17は、図16において増幅回路8を2段直列に接続して構成した回路例である。

また、図18は、図17においてノイズ発生源7と増幅回路8とミキサー回路9の各電源側に、PチャンネルMOSトランジスタQ14、Q24、Q34、Q46より成るスイッチ回路14を、また各グランド側に、NチャンネルMOSトランジスタQ11、Q21、Q31、Q41より成るスイッチ回路15を接続し

、外部からの動作許可信号 E N A B L E により、これらスイッチ回路 14、15 をオン／オフ動作し、具体的には、乱数が必要な時にのみ各回路に給電することによってジッタ生成回路 4 を作動させるように構成してある。

#### 【0048】

このように、イネーブル機能により回路の活性期間を自在に制限することで無駄な電力消費を無くし、乱数発生装置の低電力化が実現できる。

#### 【0049】

また、図 19～図 22 は、図 4 の構成に基づくジッタ生成回路 4 であり、各々ノイズ発生源 7 と増幅回路 8 の組み合わせ形態は既述した図 16～図 18 の場合と同じであるため、ここでは説明を省略する。

#### 【0050】

以上、ジッタ生成回路 4 の実施形態を説明したが、本発明では、このジッタ生成回路 4 が前記フリップ・フロップ 1 の双方の入力ライン（C L K 端子と D 端子）に付加される図 1 の乱数発生装置 10 の構成の他、このジッタ生成回路 4 をフリップ・フロップ 1 の何れか片方の入力ライン（本実施形態では、D 端子側）にのみ付加する図 2 の構成としても良く、これにより、図 1 の構成と同じ効果が得られるものである。

尚、この場合、入力端子双方の入力タイミングを合わせるため、他方の入力ライン（本実施形態では C L K 端子）にはジッタ生成回路 4 による遅延時間を補正するための R C 積分回路 13（図 3 の積分回路 12 の時定数に相当する）が付加される。

#### 【0051】

ところで、ジッタ生成回路 4 において、ミキサー回路 9 の出力には、積分波形入力によってチャタリングが発生し、フリップ・フロップ 1 の入力端子に 1 回の乱数生成周期内に複数回の入力信号が入力されてしまう不都合が生じる。

#### 【0052】

そこで、本実施形態では、図 23、図 24 に示すように、ジッタ生成回路 4 の後段に C L K 信号の両縁（立ち上がり／立ち下がり）で動作（セット／リセット）する R－S フリップ・フロップ 11 を設け、ミキサー回路 9 の出力 O U T を C

KL信号でラッチするようにした。これにより、フリップ・フロップ1にはチャタリングのない信号を入力することができ、安定した乱数の生成が行える。尚、図24の構成では、積分回路13についても後段のバッファ出力にチャタリングが発生するため、R-Sフリップ・フロップ11を付加してある。

#### 【0053】

以上説明した実施形態では、乱数発生用のフリップ・フロップ1として、Dタイプフリップ・フロップ1を用いたが、本発明はこれにのみ限定されるものではなく、これと同等の機能を有するフリップ・フロップであれば良く、例えば、R-Sフリップ・フロップを使用することもできる。

#### 【0054】

次に本発明の第2実施形態を説明する。

図25に示すように、第2実施形態の乱数発生装置10は、1bitのシリアル乱数RNDを出力するDタイプフリップ・フロップ18と、2系統の遅延回路2、3と、位相-電圧変換回路17と、図示しない位相制御回路5（図1，図2参照）とで構成されている。

#### 【0055】

ここで、前記位相-電圧変換回路17は、遅延回路2、3の遅延出力信号の位相差を電圧に変換する回路で、図26の内部回路に示すように、入力IN（CLK）と入力IN（D）の位相差を検出するゲート回路と、各ゲート回路出力によりオン／オフするPチャンネルMOSトランジスタQ2とNチャンネルMOSトランジスタQ1の直列回路と、その出力側に接続されたRC積分回路で構成されている。

#### 【0056】

上記構成の位相-電圧変換回路17は、図27（a）のように、IN（D）の位相がIN（CLK）より進んでいる場合は、その位相差分だけPチャンネルMOSトランジスタQ2をオン（この間、NチャンネルMOSトランジスタQ1はオフ）にして抵抗Rを介してコンデンサCを充電し、バッファの入力電圧 $v(t_h)$ を上昇させるように動作する。また、図27（b）のように、IN（D）の位相がIN（CLK）より遅れている場合は、その位相差分だけNチャンネルM

OSトランジスタQ1をオン（この間、PチャンネルMOSトランジスタQ2はオフ）にして抵抗Rを介してコンデンサCを放電し、バッファの入力電圧V（t<sub>h</sub>）を降下させるように動作する。

#### 【0057】

従って、この位相－電圧変換回路17の出力には、これに接続されるバッファのスレッシュホールド電圧にほぼ等しい電圧V（t<sub>h</sub>）が発生し、二つの入力、IN（CLK）とIN（D）位相差で生じるこの出力電圧の変動がバッファのスレッシュホールド電圧との関係によりデジタル信号化されてフリップ・フロップ18のD端子に入力され、出力にCLK信号に同期した1bitの乱数データRNDが得られる。そして、この乱数データRNDが前記位相制御回路5によって監視され、フリップ・フロップ出力の1または0の出現率が一定（例えば、50%）になるように二つの入力信号の位相差（即ち、位相－電圧変換回路7の出力）が自動調整される。

#### 【0058】

また、図示しないが、図25において、RC積分回路の後に抵抗を直列に接続することにより、抵抗の発する雑音がV（t<sub>h</sub>）の変動による次段素子のスレッシュホールド動作をより効果的にする。

#### 【0059】

尚、図25では、位相－電圧変換回路17とフリップ・フロップ18の間にバッファを介在したがバッファを介さずに直接フリップ・フロップ18のD端子に接続しても良い。この場合は、位相－電圧変換回路7の出力電圧V（t<sub>h</sub>）がほぼD端子のスレッシュホールド電圧に自動調整されることになる。

また、前記バッファの代わりにコンパレータを用い、この出力電圧V（t<sub>h</sub>）と基準電圧の比較によりデジタル信号を得るように構成しても良い。

#### 【0060】

また、図28に示すように、位相－電圧変換回路7の直列トランジスタ回路にPチャンネルMOSトランジスタQ4とNチャンネルトランジスタQ5を付加し、外部からの動作許可信号ENABLEにより必要時以外は回路動作を停止することにより、低電力化が図れる。

## 【0061】

図29は、位相－電圧変換回路17の出力側にジッタ生成回路4を接続した構成である。尚、このジッタ生成回路4は、ノイズ発生源7と増幅回路8とミキサ回路9とから構成される既述した図3、図4の構成であり、ここではその説明は省略する。

ジッタ生成回路4を接続し、スレッシュホールド電圧 $V(t_h)$ にジッタを生じさせることにより、フリップ・フロップ出力の1または0が出る確率の不確定要素が積極的に増加され、これにより、一様性を有し、且つ規則性や相関性や周期性を有しないより完全な自然乱数を容易に生成することができるようになる。

次に本発明の第3実施形態を説明する。

図30に示すように、第3実施形態の乱数発生装置は、1bitのシリアル乱数RNDを出力するR－Sフリップ・フロップ16と、このR－Sフリップ・フロップ16のS端子とR端子に接続される遅延回路2、3と、図示しない位相制御回路5（図1、図2参照）とで構成されている。

## 【0062】

ここで、図31はNチャンネルMOSトランジスタとPチャンネルMOSトランジスタで構成した前記R－Sフリップ・フロップの内部回路を示しており、トランジスタQ1～Q4によりS側のNANDゲート回路が、またトランジスタQ5～Q8によりR側のNANDゲート回路が構成されている。

## 【0063】

例えば、R－Sフリップ・フロップのようなエッジトリガ型のフリップ・フロップでは、S側入力信号とR側入力信号の立ち上がりの位相差を0に近づけるとメタステーブル現象が発生することが知られており、この現象が発生するとフリップ・フロップ出力が確定するまでに時間を要し、一定時間後の出力状態は、0か1、またはスレッシュホールド電圧を保持、または発振状態の何れかとなる。本実施形態は、このメタステーブル現象を積極的に利用して自然乱数を生成するものである。

## 【0064】

即ち、本実施形態では、図32に示すように、図31の回路構成において、S



側のNANDゲート回路の電源Vcc側にPチャンネルMOSトランジスタQ10を、またGND側にNチャンネルMOSトランジスタQ9を各々直列に接続すると共に、これらトランジスタQ9、Q10のゲートにノイズ発生源7と増幅回路8を接続し、当該増幅ノイズ信号によりS側のNANDゲート回路のスレッシュホールド電圧を変化するように構成した。尚、端子Sには遅延回路2の出力が、端子Rには遅延回路3の出力が接続される。また、図33は、S側、R側双方のNANDゲート回路に上記回路を付加し、それぞれに別々の増幅ノイズ信号を入力するように構成したものである。

#### 【0065】

上記構成において、NANDゲート回路のスレッシュホールド電圧を変化することにより、フリップ・フロップ出力をメタステーブル状態より即時に1または0の安定した状態にすることができる。そして、乱数データRNDが前記位相制御回路5によって監視され、フリップ・フロップ出力の1または0の出現率が一定（例えば、50%）になるように二つの入力信号の位相差が自動調整される。

#### 【0066】

以上説明した第3実施形態では、乱数発生用のフリップ・フロップ（メタステーブル現象を起こさせるフリップ・フロップ）としてR-Sフリップ・フロップ16を用いたが、本発明はこれのみに限定されるものではなく、これ以外のフリップ・フロップ（例えば、Dタイプフリップ・フロップ等）で同等の機能を実現することも勿論可能である。

#### 【0067】

また、図示しないが、既述した第1～第3実施形態のシリアル型の乱数発生装置10をP個並列に配置することにより、個々の乱数発生装置10間の相互関係が一切存在しないPbit構成の並列型乱数発生装置を構成することができる。

#### 【0068】

さらに、上記したシリアル型の乱数発生装置や並列型乱数発生装置を用いて確率発生装置を構成すれば、規則性、相関性、周期性を有さない理想的な確率を生成することができる。

#### 【0069】

以上のように、本発明の各回路は、MOSトランジスタを使用してデジタル構成したので、LSI化への対応が容易で生産性に優れ、科学技術計算、ゲーム機、暗号処理等、ハイテク産業への用途に対して大量の乱数および確率データを高速に、且つ、安価に供給することができるものである。

#### 【0070】

##### 【発明の効果】

以上説明したように、本発明によれば、乱数を生成するフリップ・フロップの入力ラインにジッタ生成回路を付加したので、入力信号のジッタにより、フリップ・フロップの不確定動作範囲が広がるため乱数の生成を容易にし、その結果、一様性を有し、且つ規則性や相関性や周期性を有しないより完全な自然乱数の発生装置を実現することができる。

また、別の構成として、位相調整を電圧に変換し、その電圧変動を回路素子のスレッショールド電圧を利用してデジタル化することにより乱数を発生するようにしたので、一様性を有し、且つ規則性や相関性や周期性を有しないより完全な自然乱数の発生装置を実現することができる。

さらに、別の構成として、フリップ・フロップのメタステーブル現象を利用することにより乱数を発生するようにしたので、一様性を有し、且つ規則性や相関性や周期性を有しないより完全な自然乱数の発生装置を実現することができる。

#### 【0071】

また、係る構成の乱数発生装置を用いることにより、全域において一様な確率分布を有する理想的な確率発生装置を実現でき、科学技術計算、ゲーム機、或いは暗号化処理等セキュリティを有するハイテク産業への参入に対し極めて有効となる。

##### 【図面の簡単な説明】

##### 【図1】

本発明に係る乱数発生装置の第1実施形態を示す図である。

##### 【図2】

本発明の第1実施形態に係る乱数発生装置の図1とは別の構成を示す図である。

。

**【図 3】**

本発明に係るジッタ生成回路の構成を示す図である。

**【図 4】**

本発明に係るジッタ生成回路の図 3 とは別の構成を示す図である。

**【図 5】**

ジッタ生成における入出力波形を示す図である。

**【図 6】**

本発明に係るノイズ発生源の構成を示す図である。

**【図 7】**

本発明に係るノイズ発生源の図 6 とは別の構成を示す図である。

**【図 8】**

本発明に係るノイズ発生源の図 7 とは別の構成を示す図である。

**【図 9】**

本発明に係るノイズ発生源の図 8 とは別の構成を示す図である。

**【図 10】**

本発明に係るノイズ発生源の図 9 とは別の構成を示す図である。

**【図 11】**

本発明に係るノイズ発生源の図 10 とは別の構成を示す図である。

**【図 12】**

本発明に係るノイズ発生源の図 11 とは別の構成を示す図である。

**【図 13】**

本発明に係るノイズ発生源の図 12 とは別の構成を示す図である。

**【図 14】**

本発明に係る増幅回路の構成を示す図である。

**【図 15】**

本発明に係る増幅回路の図 14 とは別の構成を示す図である。

**【図 16】**

本発明に係るジッタ生成回路の回路構成を示す図である。

**【図 17】**

本発明に係るジッタ生成回路の図 16 とは別の回路構成を示す図である。

【図 18】

本発明に係るジッタ生成回路の図 17 とは別の回路構成を示す図である。

【図 19】

本発明に係るジッタ生成回路の図 18 とは別の回路構成を示す図である。

【図 20】

本発明に係るジッタ生成回路の図 19 とは別の回路構成を示す図である。

【図 21】

本発明に係るジッタ生成回路の図 20 とは別の回路構成を示す図である。

【図 22】

本発明に係るジッタ生成回路の図 21 とは別の回路構成を示す図である。

【図 23】

ラッチ回路を付加した本発明に係る乱数発生装置の要部回路図である。

【図 24】

ラッチ回路を付加した本発明に係る乱数発生装置の図 23 とは別の要部回路図である。

【図 25】

本発明に係る乱数発生装置の第 2 実施形態を示す図である。

【図 26】

本発明に係る位相－電圧変換回路を示す図である。

【図 27】

図 26 の位相－電圧変換回路の動作を示す図である。

【図 28】

本発明に係る位相－電圧変換回路の図 26 とは別の構成を示す図である。

【図 29】

本発明の第 2 実施形態に係る乱数発生装置の図 25 とは別の構成を示す図である。

【図 30】

本発明に係る乱数発生装置の第 3 実施形態を示す図である。

**【図 3 1】**

R－S フリップ・フロップの内部構成を示す図である。

**【図 3 2】**

本発明の第 3 実施形態に係る R－S フリップ・フロップの内部構成を示す図である。

**【図 3 3】**

本発明の第 3 実施形態に係る図 3 2 とは別の R－S フリップ・フロップの内部構成を示す図である。

**【図 3 4】**

D タイプフリップ・フロップを示す図である。

**【図 3 5】**

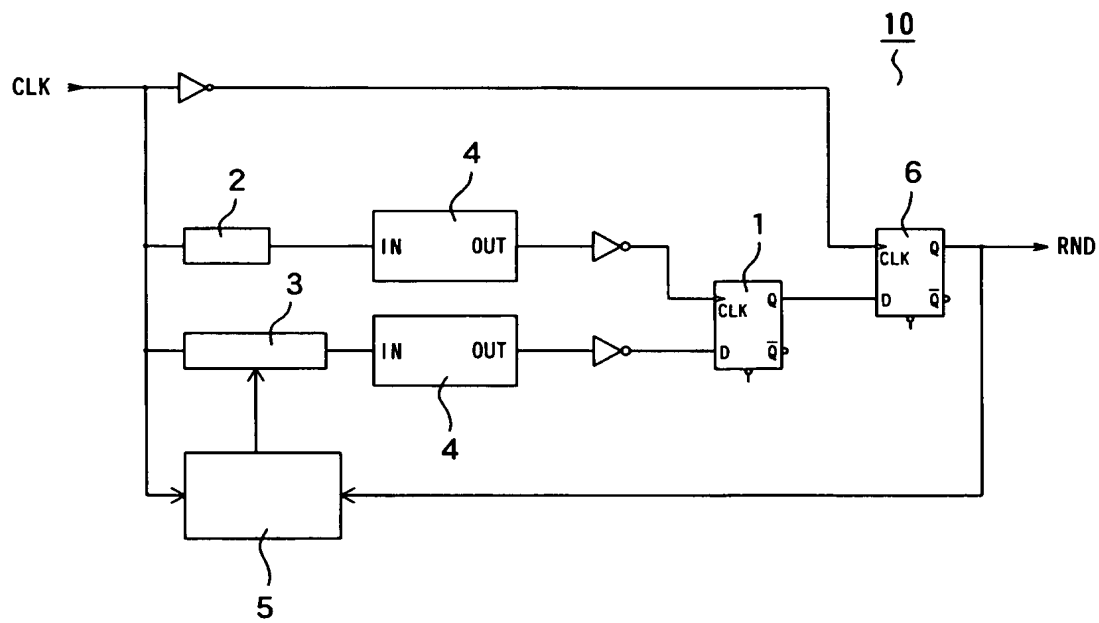
図 3 4 のフリップ・フロップの動作を示す図である。

**【符号の説明】**

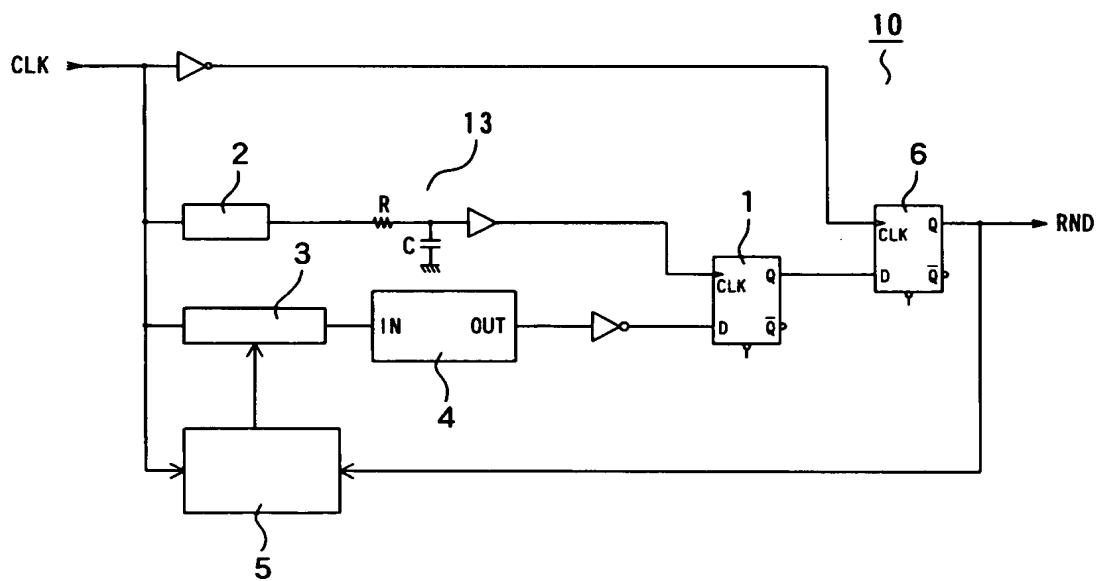
- 1    フリップ・フロップ
- 4    ジッタ生成回路
- 7    ノイズ発生源
- 8    増幅回路
- 9    ミキサー回路
- 10   乱数発生装置
- 11   ラッチ手段（R－S フリップ・フロップ）
- 12, 13   積分回路
- 14, 15   イネーブル手段（スイッチ回路）
- 16   R－S フリップ・フロップ
- 17   位相－電圧変換回路

【書類名】 図面

【図 1】

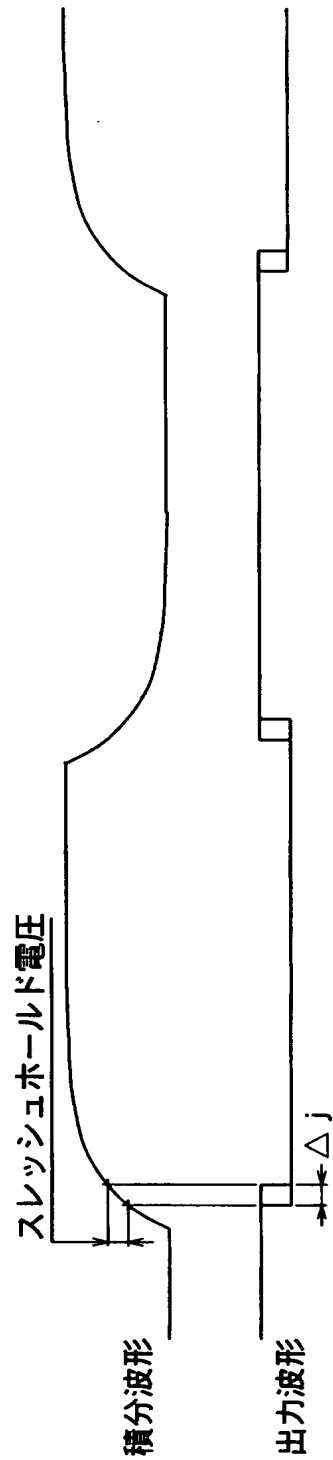


【図 2】



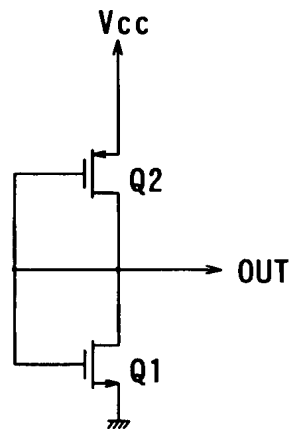


【図 5】

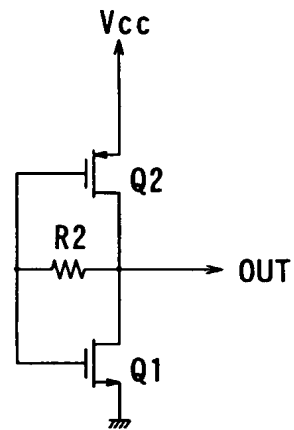




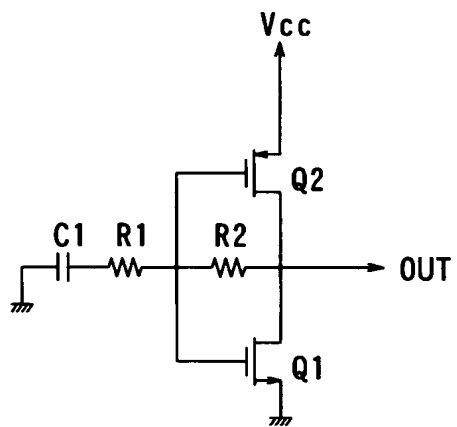
【図 6】



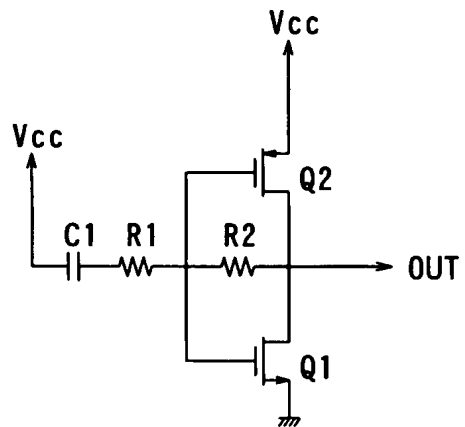
【図 7】



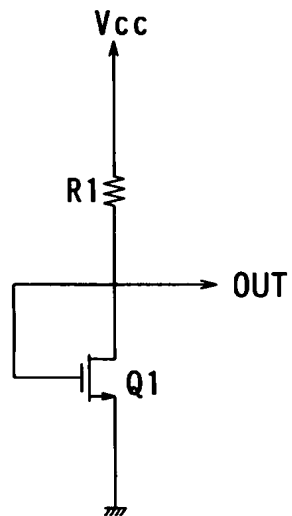
【図 8】



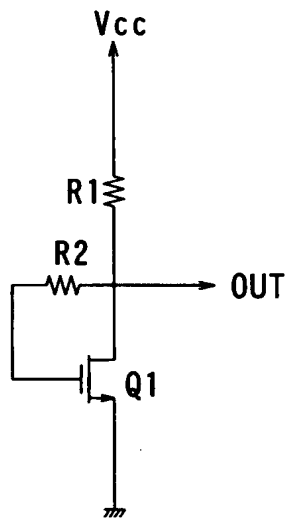
【図 9】



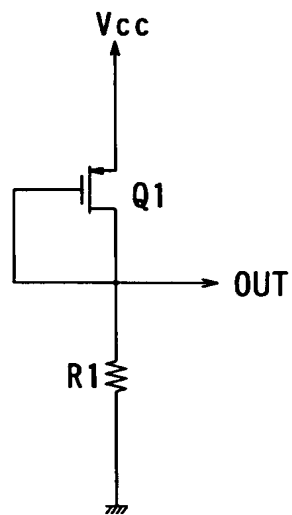
【図 10】



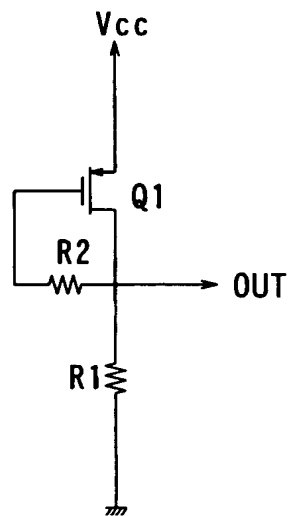
【図 1 1】



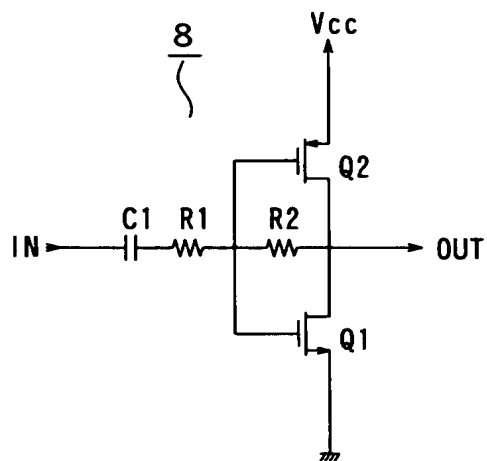
【図 1 2】



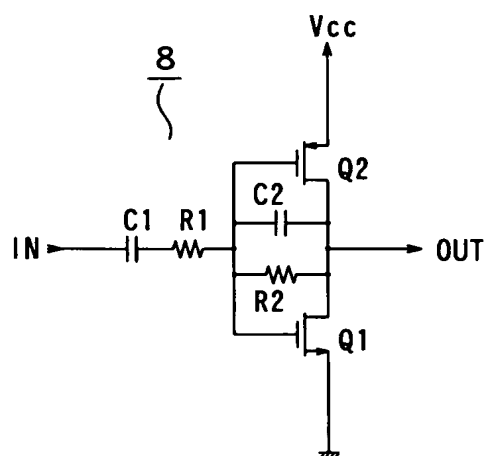
【図 13】



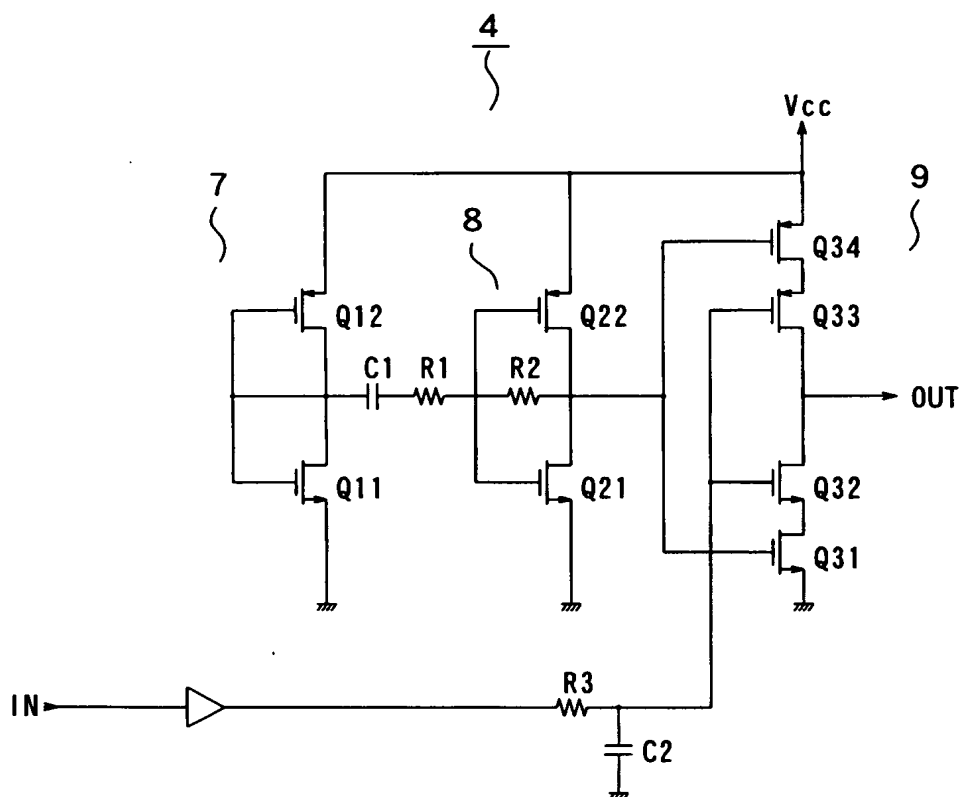
【図 14】



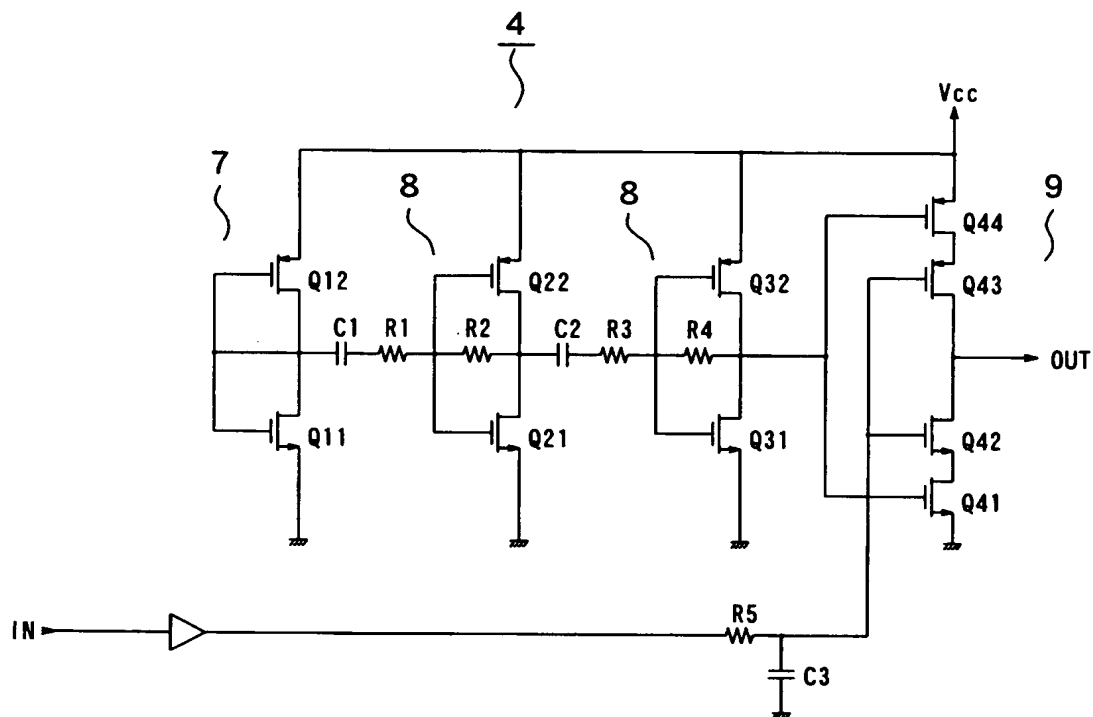
【図 15】



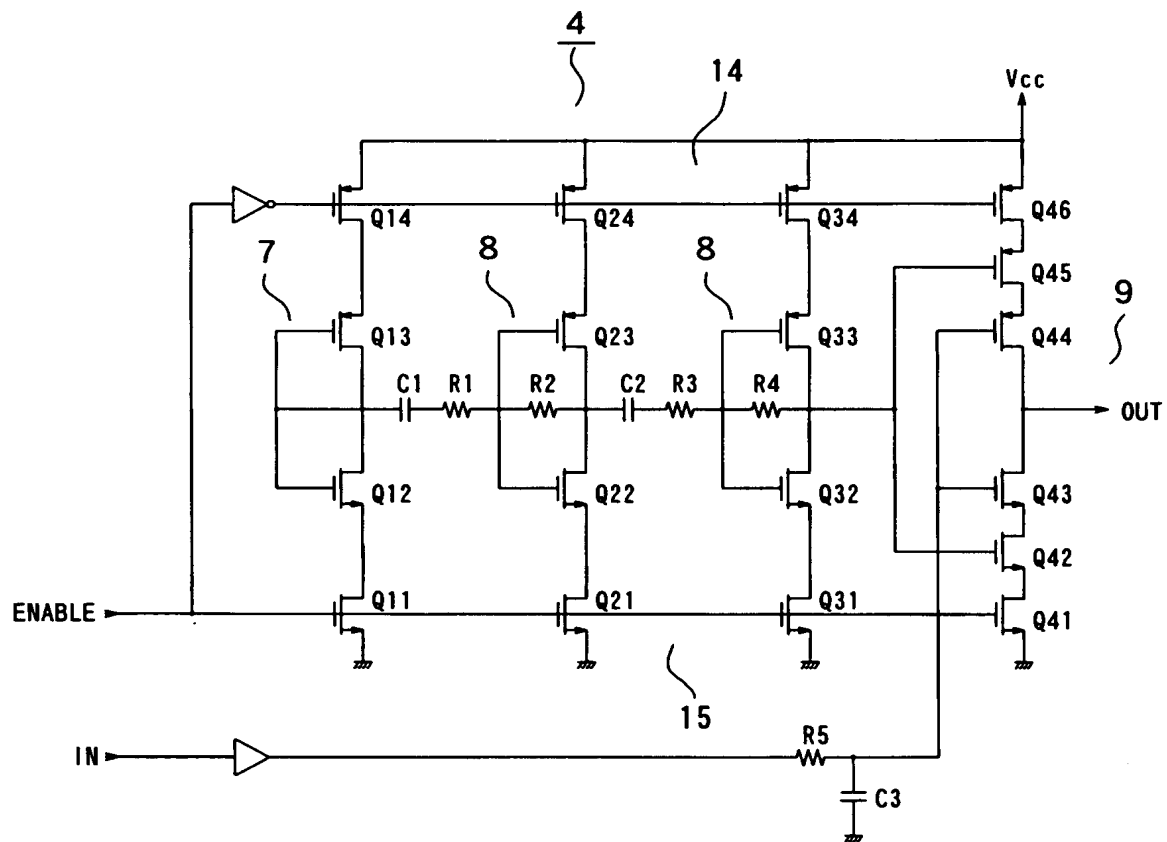
【図 16】



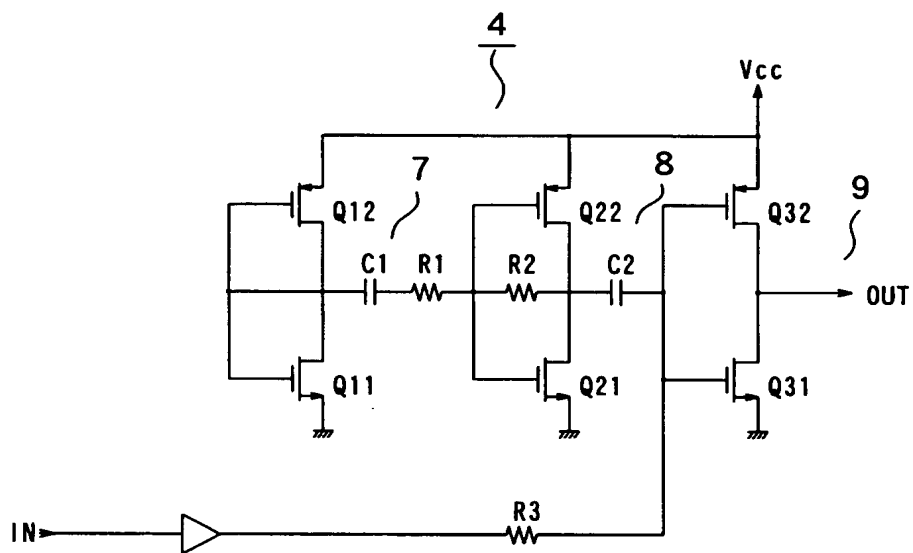
【図 17】



【図 18】

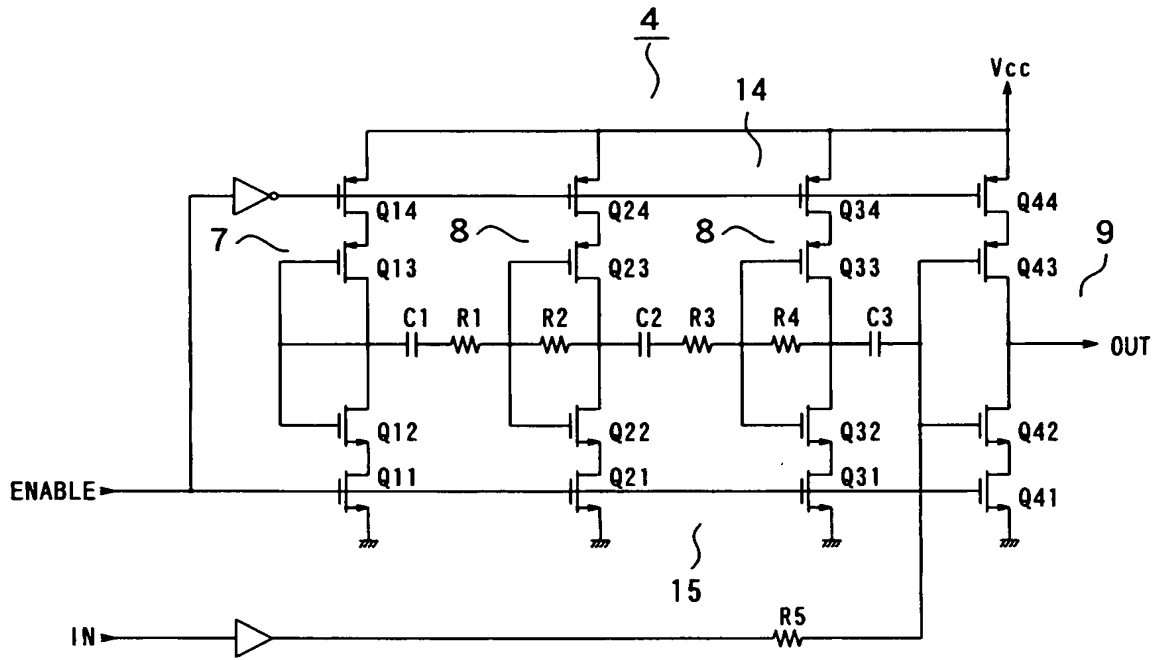


【図 19】

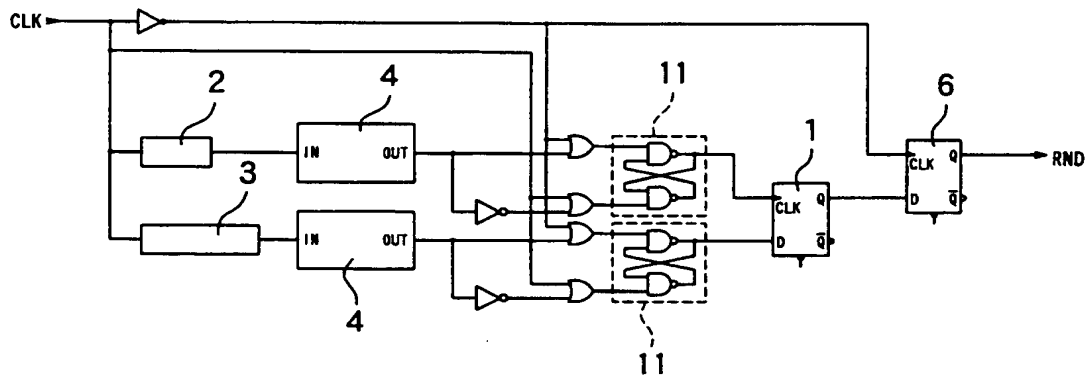




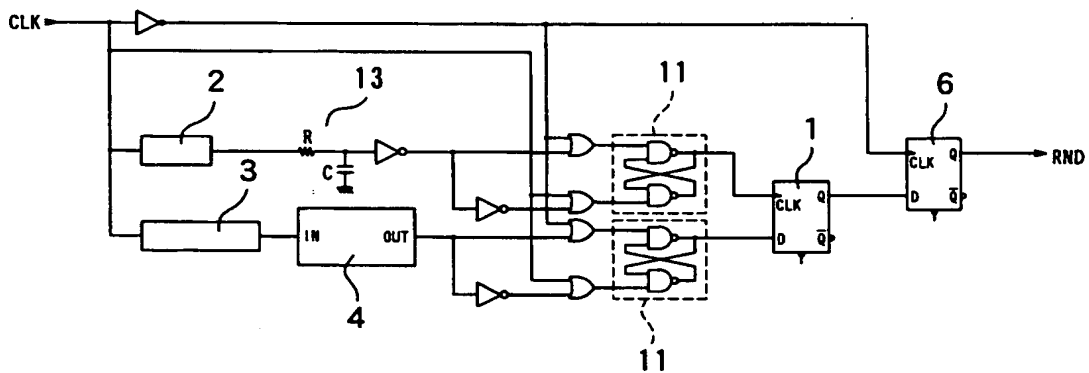
【図 2 2】



【図 2 3】

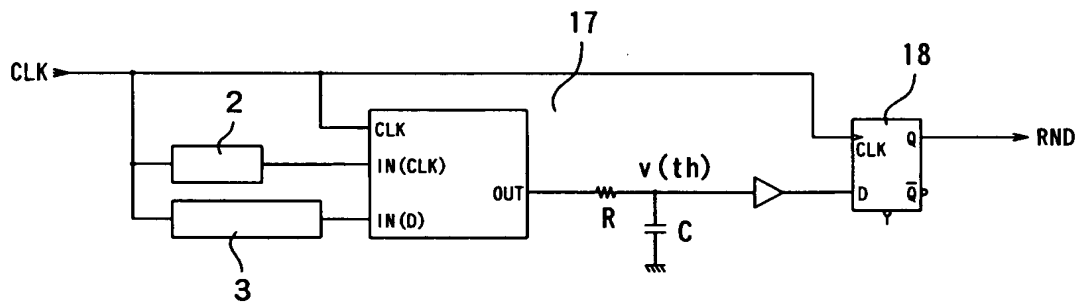


【図 2 4】

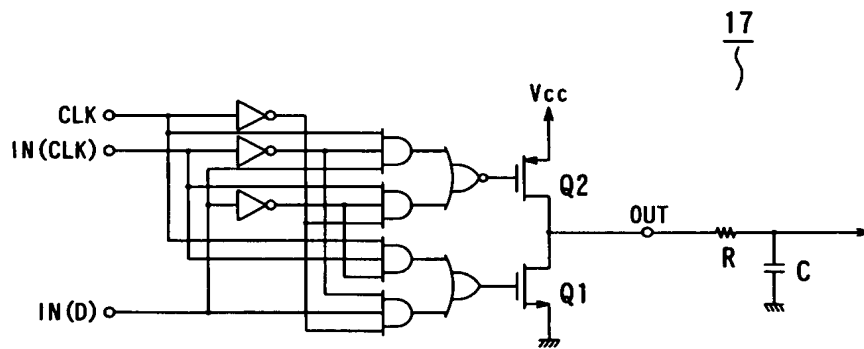




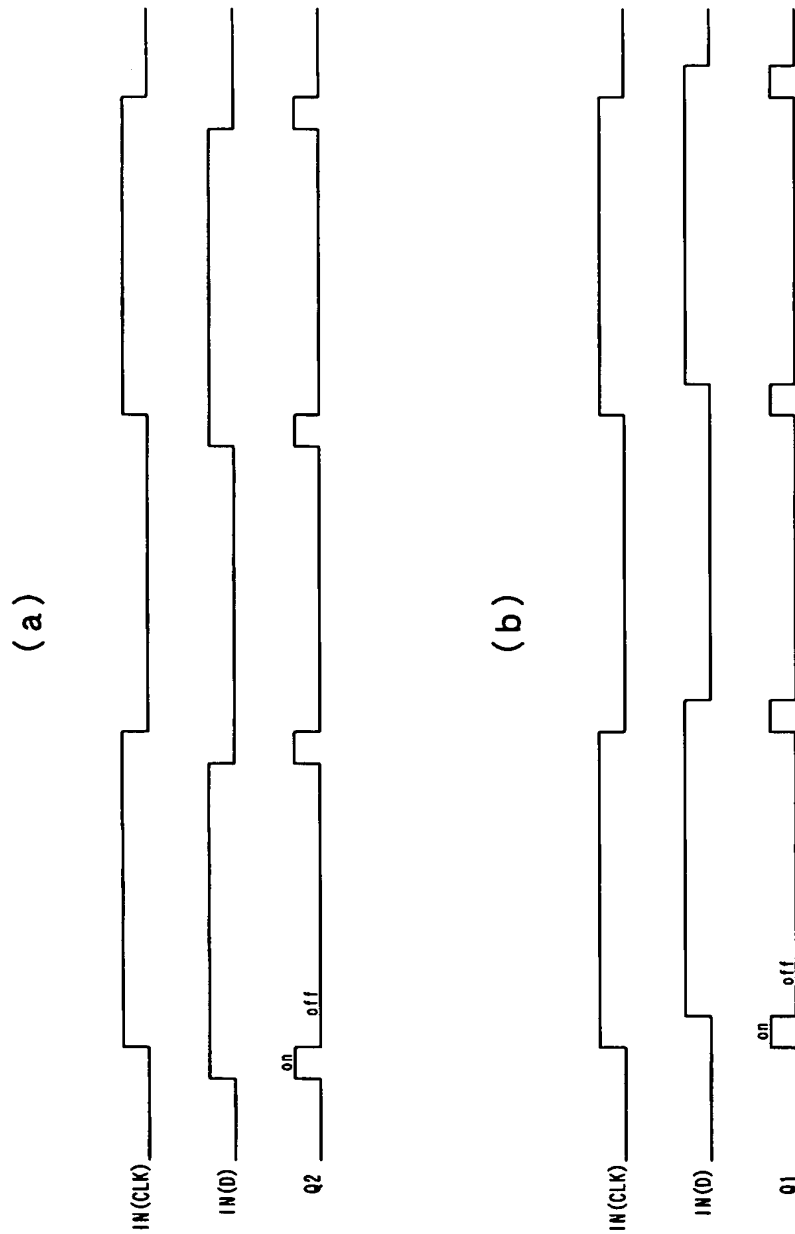
【図 25】



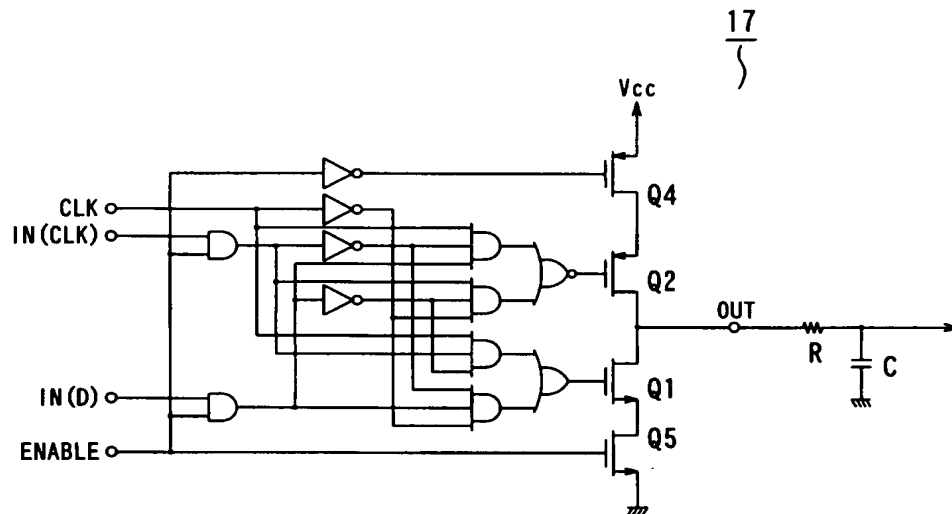
【図 26】



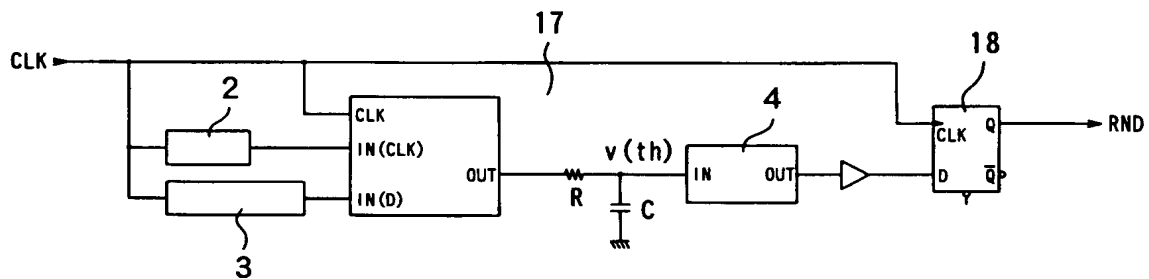
【図 27】



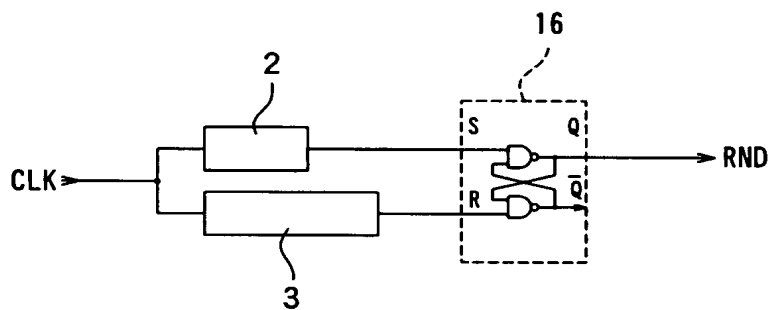
【図 28】



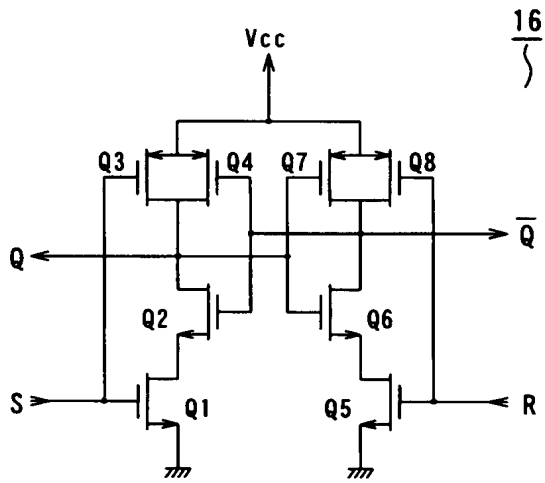
【图 29】



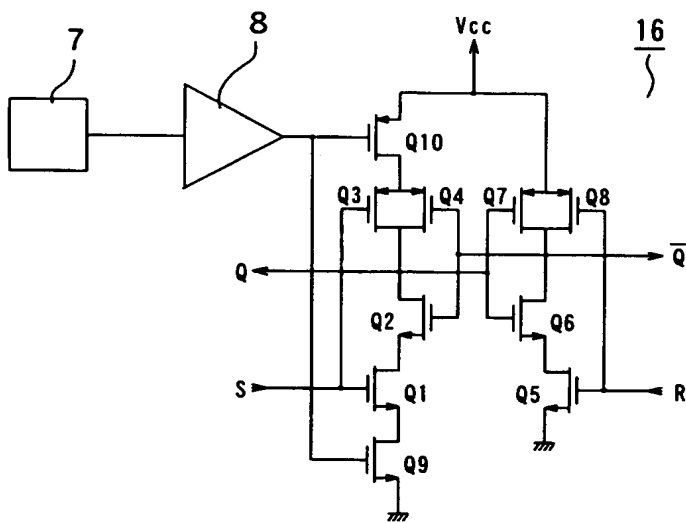
【図 30】



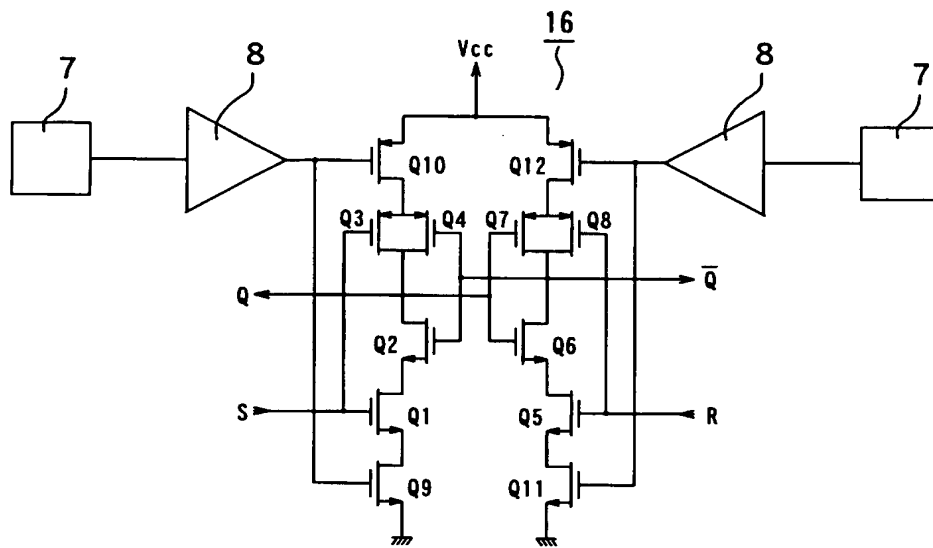
【図 3 1】



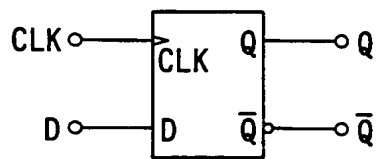
【図 3 2】



【図 3 3】

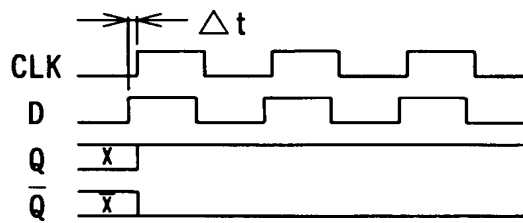


【図 3 4】

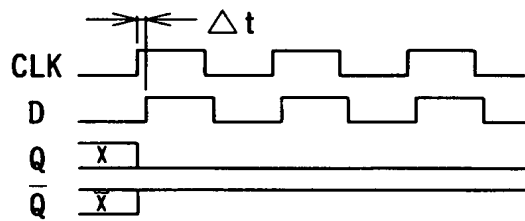


【図 35】

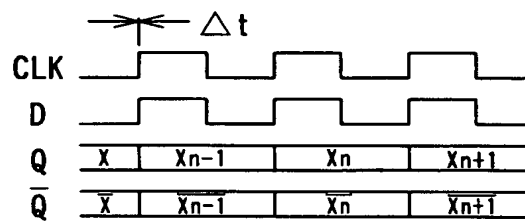
(a)



(b)



(c)



【書類名】 要約書

【要約】

【課題】 回路規模が小さく小型化、薄型化で L S I 搭載に適し、生産性に優れ安価に作製できると共に、一様性を有し規則性や相関性や周期性を有しないより完全な乱数発生装置および確率発生装置を提供する。

【解決手段】 フリップ・フロップに入力する二つの入力信号の位相を自動調整してフリップ・フロップ出力の 1 または 0 の出現率を一定に維持する乱数発生装置 1 0 において、前記フリップ・フロップ 1 の入力信号ラインに、ノイズ発生源と、当該ノイズを増幅する増幅回路と、増幅ノイズ信号と前記入力信号を入力して入力信号にジッタを生じさせるミキサー回路とから成るジッタ生成回路 4 を付加した。本構により、入力信号にジッタが発生し、フリップ・フロップ 1 の不確定動作範囲が広がる。これにより一様性を有し、規則性や相関性や周期性を有しないより完全な自然乱数を容易に生成することができる。

【選択図】 図 1

認定・付加情報

特許出願の番号	特願 2 0 0 1 - 1 7 0 9 4 5
受付番号	5 0 1 0 0 8 1 6 3 9 1
書類名	特許願
担当官	第八担当上席 0 0 9 7
作成日	平成 1 3 年 6 月 7 日

<認定情報・付加情報>

【提出日】	平成13年 6月 6日
-------	-------------

次頁無



特願 2 0 0 1 - 1 7 0 9 4 5

出 願 人 履 歴 情 報

識別番号

[ 3 9 0 0 2 2 7 9 2 ]

1 . 変 更 年 月 日

1 9 9 0 年 1 1 月 1 3 日

[ 変 更 理 由 ]

新 規 登 録

住 所

東 京 都 港 区 新 橋 5 丁 目 3 6 番 1 1 号

氏 名

い わ き 電 子 株 式 会 社